Disclaimer:
This English translation is produced by machine translation and may contain errors.The JPO, the INPIT, and and those who drafted this document in the original language are not responsible for the result of the translation.

Notes:
1. Untranslatable words are replaced with asterisks (****).
2. Texts in the figures are not translated and shown as it is.

Translated: 04:38:59 JST 07/21/2007
Dictionary: Last updated 07/20/2007 / Priority: 1. Information communication technology (ICT) / 2. Electronic engineering / 3. JIS (Japan Industrial Standards) term

FULL CONTENTS

[Claim(s)]
[Claim 1] The IC card which has non-volatile memory, and the data stored in this IC card are read. Consist of read/write equipment which performs application using the data, and two or more lock data common to both is stored in the non-volatile memory of said IC card and read/write equipment. In the IC card system which performs access privilege control of the data in an IC card, or uses this common lock data for the communication data encryption / decoding between an IC card and read/write equipment The lock data field and two or more application-data fields of plurality [non-volatile memory / of said IC card], The IC card system characterized by having prepared the correspondence table showing correspondence with these lock data and an application data, and preparing two or more lock data fields, the correspondence table prepared at said IC card, and the same correspondence table in the non-volatile memory of said read/write equipment.
[Claim 2] The IC card system with which the number of lock data is characterized by the number of application datas, and an inharmonious thing in an IC card system according to claim 1.
[Claim 3] The IC card which has non-volatile memory, and the data stored in this IC card are read. Consist of read/write equipment which performs application using the data, and two or more common lock data common to both is stored in the non-volatile memory of said IC card and read/write equipment. In the IC card system which performs access privilege control of the data in an IC card, or uses this common lock data for the communication data encryption / decoding between an IC card and read/write equipment The correspondence table with which two or more pointers to one lock data field and this lock data field were stored in the non-volatile memory of said IC card corresponding to the application data is prepared. The IC card system characterized by preparing the same correspondence table as one lock data field and the correspondence table prepared in said IC card in the non-volatile memory of said read/write equipment.
[Claim 4] The IC card system with which the number of the pointers to a lock data field is characterized by the number of application datas, and an inharmonious thing in an IC card system according to claim 3.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention is a thing about the IC card system which consists of an IC card and read/write equipment. It has the feature in the IC card in the case of holding the key for setting an access privilege as the data in an IC card especially, or enciphering in common to an IC card and the read/write equipment which counters, and the composition of read/write equipment.
[0002]
[Description of the Prior Art] [the lock data used in order to give an access privilege conventionally to the data stored in an IC card or to encipher the data in an IC card] It was decided, respectively at the time of issue of an IC card that 1 to 1 would be an application-data field, and said lock data was stored in the management area of an application-data field. As a method of making a lock data field and an application-data field corresponding to 1 to 1, it has the table to which the start address of a lock data field and an application area was made to correspond fixed in the non-volatile memory in an IC card at the time of issue, and this relation could change after issue no longer.

[0003] Between the IC card by a Prior art, and read/write equipment, the correspondence relation of the procedure, lock data field, and application area in the case of canceling the access privilege of an IC card is shown in drawing 6 . Moreover, the key modification procedure by the conventional method is shown in drawing 7 . In drawing 6 , 100A is conventional read/write equipment and has following each part. That is, 101 is a lock data field and each lock data of KD1, KD2, ..., KDn is stored. As for the lock data read-out means against the address 103A wants to carry out read/write, and 105, an error-processing means and 107 are application execution means the lock data index KIDi (i= 1, 2, --, n) and lock data KDi-T for verification, and 106.

[0004] 200A is the conventional IC card and consists of following each part. Namely, the application-data field where security protection of 201 was carried out with the key, A lock data field and 204 202 The receiving means of the information from said read/write equipment 100A, NG response sending-out means and 210 are O.K. response sending-out means the right of a lead of the application data AD corresponding to the lock data KD in 208 corresponding to a lock data comparison means in 206 corresponding to the lock data read-out means from a lock data index in 205 or the Rheydt right grant means, and 209. The IC card system consisted of above-mentioned read/write equipment 100A and IC card 200A.

[0005] Next, operation of the conventional IC card system of drawing 6 is explained using the flow chart of drawing 7 . In addition, - (S41) in drawing 7 (S52) shows each step.

[0006] Key change preparations of an IC card are made by the read/write equipment 100A side (S41). New lock data KDi-T corresponding to the application data ADi in the application-data field 201 by which security protection was carried out with the key of IC card 200A is set to a key change command (S42).

[0007] The lock data index KIDi and new lock data KDi-T to change are transmitted with a key change command (S43).

[0008] Next, the lock data index KIDi and new lock data KDi-T are received by the IC card 200A side (S44), and, subsequently new lock data KDi-T is written in the lock data field corresponding to the lock data index KIDi by overwrite (S45). If it confirms whether it was able to write normally (S46) and can be writing normally, it will transmit by O.K. response (S47). It reads because read/write equipment 100A receives this O.K. response, and preparation is completed (S48), and it progresses to the next key rewriting (S49). At a step (S46), in the case of NG, NG response is transmitted (S50), this NG response is received (S51), and read/write equipment 100A progresses to error processing (S52). By the above-mentioned conventional method, when lock data was changed, only the number of the lock data to change needed to transmit the command of key change which set new lock data.

[0009]

[Problem to be solved by the invention] For this reason, when the lock data KD in IC card 200A needs to be changed for a certain Reason, it is necessary to change the lock data storing pointer stored in each application-data field 201, and the lock data after change using a key change command. It is necessary to match the lock data field 202 with the application-data field 201 beforehand 1 to 1 at the time of issue of IC card 200A, and the memory space which the lock data KD occupies depends for it on the length of the lock data decided at the time of issue. For this reason, after issue ended, when it was going to change the length of lock data, the correspondence relation between the lock data field 202 and the application-data field 201 had to be improved again, and the recurrence line had to be performed.

[0010] When it was made in order that this invention might solve these problems, and the purpose changes lock data by communication between an IC card and read/write equipment The length of lock data is easily changed a change front and after change, or it is in enabling it to change lock data simply so that it is not necessary to change one lock data at a time with a key change command.

[0011]

[Means for solving problem] The IC card in which invention according to claim 1 concerning this invention has non-volatile memory, Read the data stored in this IC card, and it consists of read/write equipment which performs application using that data. Two or more common lock data is stored in the non-volatile memory of said IC card and read/write equipment in both. In the IC card system which performs access privilege control of the data in an IC card, or uses this common lock data for the communication data encryption / decoding between an IC card and read/write equipment The lock data field and two or more data areas for applications of plurality [non-volatile memory / of an IC card], The same correspondence table as the correspondence table which prepared the correspondence table showing correspondence with these lock data and an application data, and was prepared in two or more lock data fields and IC cards at the non-volatile memory of read/write equipment is prepared.

[0012] Moreover, the number of lock data makes invention according to claim 2 the number and inequality of an application data.
[0013] Invention according to claim 3 reads the IC card which has non-volatile memory, and the data stored in this IC card. Consist of read/write equipment which performs application using the data, and two or more common lock data common to both is stored in the non-volatile memory of said IC card and read/write equipment. In the IC card system which performs access privilege control of the data in an IC card, or uses this common lock data for the communication data encryption / decoding between an IC card and read/write equipment The correspondence table with which two or more pointers to one lock data field and lock data field were stored in the non-volatile memory of an IC card corresponding to the application data is prepared. The same correspondence table as one lock data field and the correspondence table prepared in the IC card is prepared in the non-volatile memory of read/write equipment.
[0014] Moreover, the number of the pointers to a lock data field makes invention according to claim 4 the number and inequality of an application data.
[0015]
[Mode for carrying out the invention] [invention according to claim 1 in the IC card system concerning this invention] When changing the key for every application-data field between an IC card and read/write equipment, it is not necessary to communicate in the lock data after change itself, and since only the number after change of a correspondence table is communicated, lock data can be changed easily.
[0016] Since the number of lock data and the number of application datas are not 1 to 1, the analogy of lock data becomes difficult to carry out invention according to claim 2, and it can aim at memory saving of a lock data field easily.
[0017] When changing the key for every application-data field between an IC card and read/write equipment, the invention of Claim 3 does not need to communicate in the lock data after change itself, and since it should communicate only the pointer after change of a correspondence table, it can change lock data easily.
[0018] Since the number of the pointers to a lock data field and the number of application datas are not 1 to 1, the analogy of lock data becomes difficult to carry out invention of Claim 4, and it can aim at memory saving of a lock data field easily.
[0019]
[Working example] The composition of one work example of this invention is shown in the block diagram of drawing 1 . In drawing 1 , the same sign is given to the same portion as drawing 6 . In drawing 1 , 100 is read/write equipment and has following each part. That is, 101 is a lock data field and each lock data of KD1, KD2, ..., KDn is stored. The correspondence table of the lock data and the address which explain 102 in full detail behind, the correspondence table reference means against the address data AD to carry out read/write of 103 to, As for a lock data read-out means by which 104 corresponds, and 105, an error-processing means and 107 are application execution means a lock data index and the lock data for verification, and 106. 200 is an IC card and has following each part. Namely, the application-data field where security protection of 201 was carried out with the key, 202 a lock data field and 203 a correspondence table and 204 The receiving means of the information from read/write equipment 100, 205 The read-out means of the lock data KD from a lock data index, NG response sending-out means and 210 are O.K. response sending-out means the right of a lead of the address corresponding to lock data (KD) in 208 corresponding to a correspondence table reference means in 207 corresponding to a lock data comparison means in 206 or the Rheydt right grant means, and 209.
[0020] Drawing 2 is a figure explaining the composition of the correspondence table 203 (correspondence table 102 of read/write equipment 100) of IC card 200. It is the correspondence table of the lock data index KIDi (i= 1, 2, ..., n) and the application-data index AIDi (i= 1, 2, ..., n).
[0021] Moreover, drawing 3 shows the work example of the correspondence table 203 (102) at the time of using a pointer. KDP1, KDP2, ..., KDPn are the pointers to a lock data field in this figure, and the address of the lock data field is pointed out. The addresses to which it points, respectively differ. Moreover, when the lock data length from the address which a pointer shows surpasses the top address of a lock data field, it is assumed that it is connected with the lowest address.
[0022] Next, operation of the work example of drawing 1 is divided into (1) normal-operation (2) key change operation, and it explains with reference to drawing 4 and drawing 5 . In addition, = (S1) in drawing 4 (S15) and - (S21) in drawing 5 (S32) show each step.
[0023] (1) Normal operation (refer to drawing 4)

This flow of operation has described only access privilege release operation for reading (lead) and performing operation and write-in (Rheydt) operation which receives IC card 200.

[0024] First, the preparations which read the application-data field (ADi) of IC card 200 to the read/write equipment 100 side are made (S1), and the lock data index KIDi corresponding to the application data ADi of IC card 200 is taken out from the correspondence table 102 (S2). Lock data KDi-T for access privilege verification corresponding to the lock data index KIDi is taken out from the lock data field 101 (S3). The lock data index KIDi and lock data KDi-T for verification are transmitted to IC card 200, and it verifies by the verifying function of IC card 200 (S4).

[0025] The lock data index KIDi and lock data KDi-T for verification are received (S5), and parity check and the check of the code for error corrections are performed to the IC card 200 side.

[0026] Subsequently, lock data KDi-C corresponding to the lock data index KIDi is taken out from the lock data field 202 in IC card 200 (S6).

[0027] If lock data KDi-C taken out from its key data area is compared (S7), and it agrees and will not agree to the following step (S8), it moves to a step (S13). [who received] [lock data KDi-T and the one]

[0028] The application-data index AIDi of the application-data field 201 corresponding to the lock data index KIDi is taken out from the correspondence table 203 in IC card 200 (S8). The access privilege to the application-data field 201 corresponding to the application-data index AIDi taken out at the step (S8) is unlocked (S9). In order to show having ended normally, O.K. response is transmitted to read/write equipment 100 (S10).

[0029] Since it turns out that the access privilege to the application data ADi of the application-data field 201 was unlocked when receiving O.K. response from IC card 200 (S11) Next, a lead write command is transmitted to IC card 200, and read-out of the data stored in the application data ADi and the data to the application-data field 201 are written in (S12).

[0030] On the other hand, in order to show having terminated abnormally at the step (S7), NG response is transmitted to read/write equipment (S13).

[0031] Since it is whether the error occurred within IC card 200, or to have given the wrong directions to IC card 200 when receiving NG response from IC card 200 (S14), it shifts to the processing means for error recovery. Since this invention is out of range, the method of error recovery is not described (S15).

[0032] In drawing 4 although the lock data index KIDi and lock data KDi-T for verification are transmitted to IC card 200 from read/write equipment 100 With reference to the correspondence table 203, you may ask for the lock data index KIDi by the application-data index AIDi within IC card 200 as an application-data index AIDi instead of the lock data index KIDi.

[0033] (2) Key change operation (refer to drawing 5)

After the correspondence table 203 by the side of IC card 200 confirms [the old table and] whether to already be changed into a new table before rewriting operation, the following rewriting operation is performed (S21).

[0034] With read/write equipment 100, a new correspondence table is created by recombination of the correspondence table 102. For example, supposing correspondence with an application-data index and a lock data index supports 1 to 1 like AID1, KID1, AID2 and KID2, and ... in the old correspondence table The new correspondence table which changed this combination like AID1, KID3, AID2 and KID1, and ... is created (S22). A new correspondence table is transmitted to IC card 200 as a correspondence table change command (S23). A new correspondence table is received as a correspondence table change command (S24). In new correspondence table reception, it checks for no error on transmission by the parity error, an error correction code, etc. (S25). When errorless and a receiving error occurs to the following step (S26), it shifts to a step (S31). If there is no receiving error in a new correspondence table, a new correspondence table is stored in the old correspondence table by overwrite (S26).

[0035] It confirms whether overwrite storing was completed normally (S27), and when writing is made normally and writing is not normally completed to the following step (S28), it shifts to a step (S31). In addition, when it terminates normally, the flag data in which it is shown that the state of a correspondence table is a new table is written in non-volatile memory.

[0036] O.K. response is transmitted in order to notify read/write equipment 100 that it has changed into a new correspondence table normally (S28).

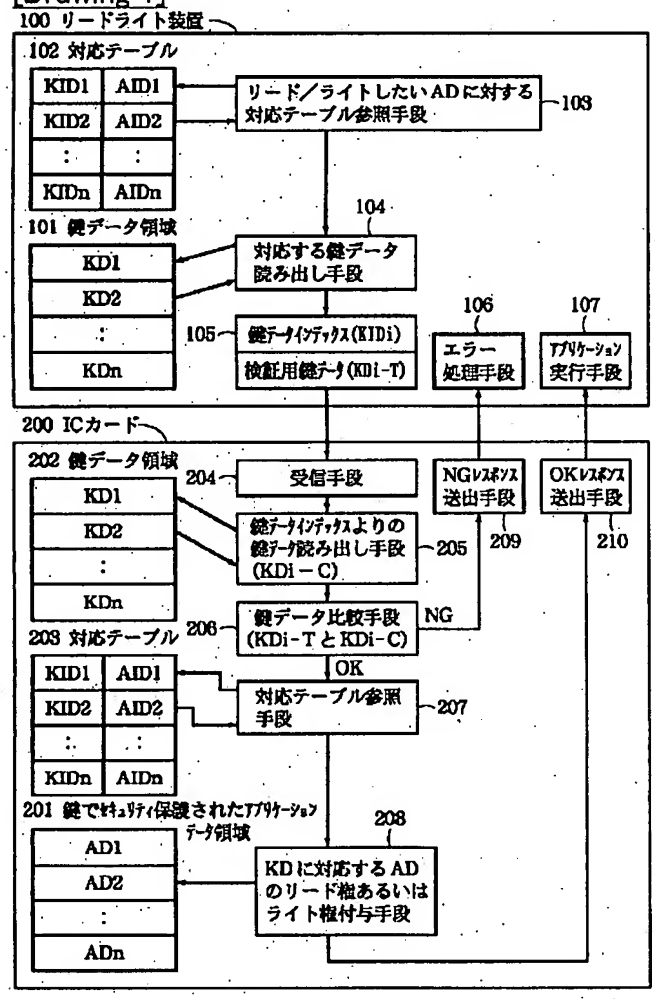
[0037] When receiving O.K. response from IC card 200, it turns out that the correspondence table by the side of IC card 200 has changed read/write equipment 100 normally (S30). (S29) Moreover, NG response is transmitted in order to show that abnormalities occurred (S31). Error processing will be performed if NG response is received

from IC card 200 (S32) (S33).
[0038]
[Effect of the Invention] The effect of this invention is as follows.
[0039] the correspondence table with which invention given in Claim 1 and 3 shows correspondence with two or more lock data fields, two or more data areas for applications, these lock data, and an application data to the non-volatile memory of an IC card -- or The correspondence table with which two or more pointers to one lock data field and lock data field were stored corresponding to the application data is prepared. Since the same correspondence table as the pointer to two or more lock data fields or lock data fields and the correspondence table in an IC card was prepared in the non-volatile memory of IC card read/write equipment When it is necessary to change lock data, it is not necessary to send the lock data itself to an IC card from IC card read/write equipment, and since change of a key can be performed only by rearranging and sending a correspondence table, lock data change of an IC card can be performed easily.
[0040] [invention given in Claim 2 and 4] since the number of lock data or the number of the pointers to a lock data field made the number of application datas inharmonious for example, when there are few application datas than the number of lock data Can choose at the time of lock data change of intact lock data, and in [that] being reverse Change of lock data can be performed by carrying out a belt using the key of a different application data. When two or more lock data fields are shared in an application-data field, the memory of an IC card is used efficiently or a margin is in the memory of an IC card, the lock data field is made more than the number of application-data fields, a key can be stored, and it can prepare for emergency.
[0041] In addition, although the example of normal operation of the work example showed the case where an access privilege was unlocked by a plaintext key, a correspondence table is applicable to combination change of all the keys used in an IC card. For example, it can be used for change of the key used for a communication data encryption etc. In this case, [by the conventional method, unless it sent the lock data itself to the IC card with the key change command, were not able to change, but] In this invention, since a key can be changed if a correspondence table is sent, a key can be changed without sending out lock data on the channel between IC card read/write equipment and an IC card, and security improves.

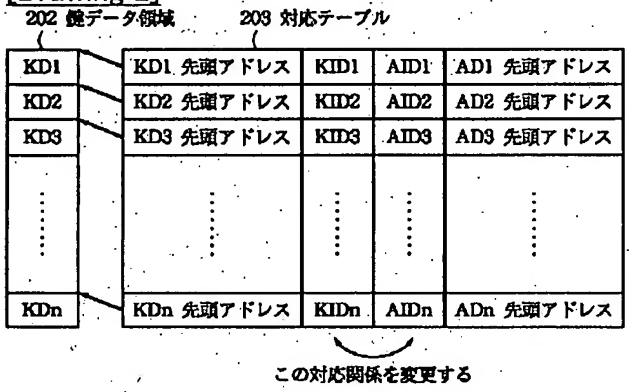
[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the composition of one work example of this invention.
[Drawing 2] It is the figure showing the example of composition of a correspondence table.
[Drawing 3] It is the figure showing other composition of a correspondence table.
[Drawing 4] It is the figure showing the flow of operation at the time of the normal operation of this invention.
[Drawing 5] It is the figure showing the flow of operation at the time of key change operation of this invention.
[Drawing 6] It is the figure showing the conventional example.
[Drawing 7] It is the figure showing the flow at the time of the conventional key change operation.
[Explanations of letters or numerals]
100 Read/write Equipment
101 Lock Data Field
102 Correspondence Table
103 Correspondence Table Reference Means against AD to Carry Out Read/write
104 Lock Data Read-out Means
105 Lock Data Index and Lock Data for Verification
106 Error-Processing Means
107 Application Execution Means
200 IC Card
201 Application-Data Field
202 Lock Data Field
203 Correspondence Table
204 Receiving Means
205 Lock Data Read-out Means
206 Lock Data Comparison Means

207 Correspondence Table Reference Means
208 Right of Lead or Rheydt Right Grant Means of Address
209 NG Response Sending-Out Means
210 O.K. Response Sending-Out Means

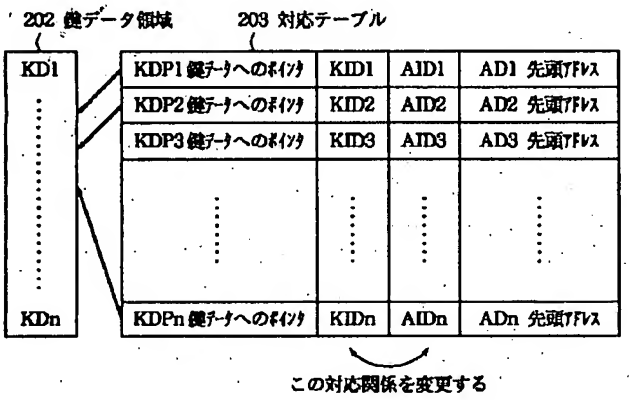
[Drawing 1]



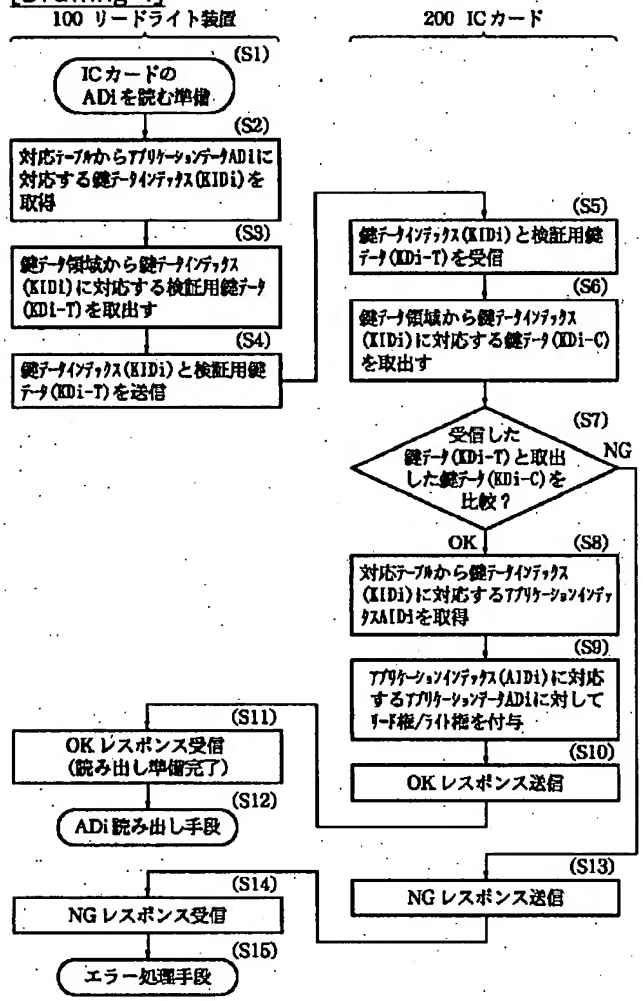
[Drawing 2]



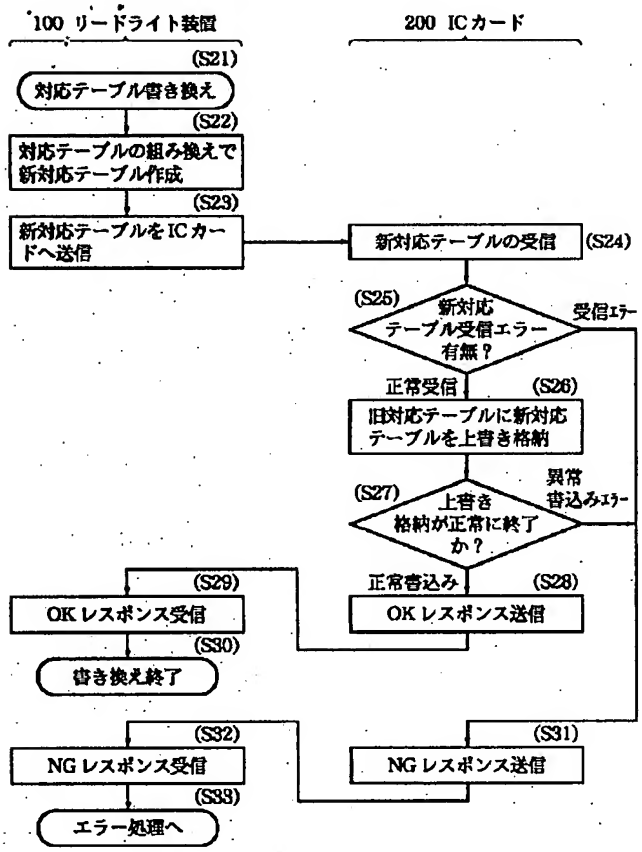
[Drawing 3]



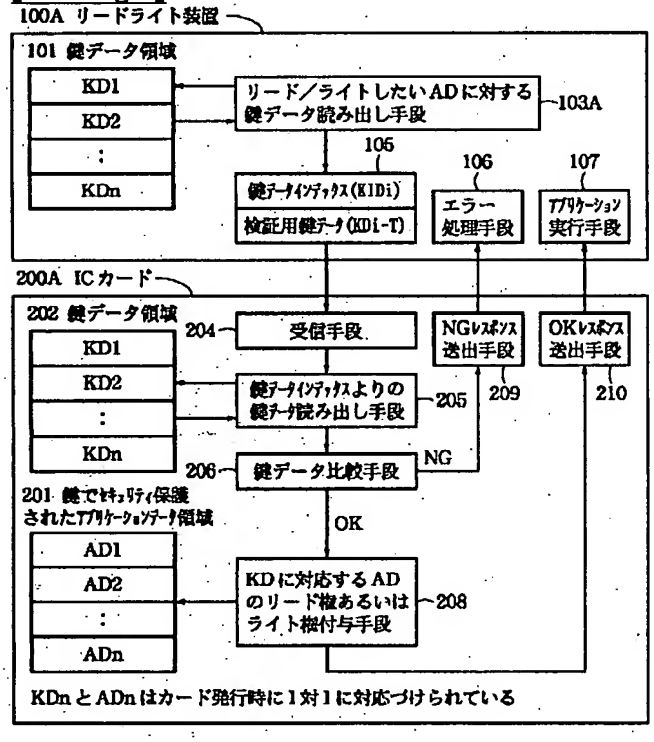
[Drawing 4]



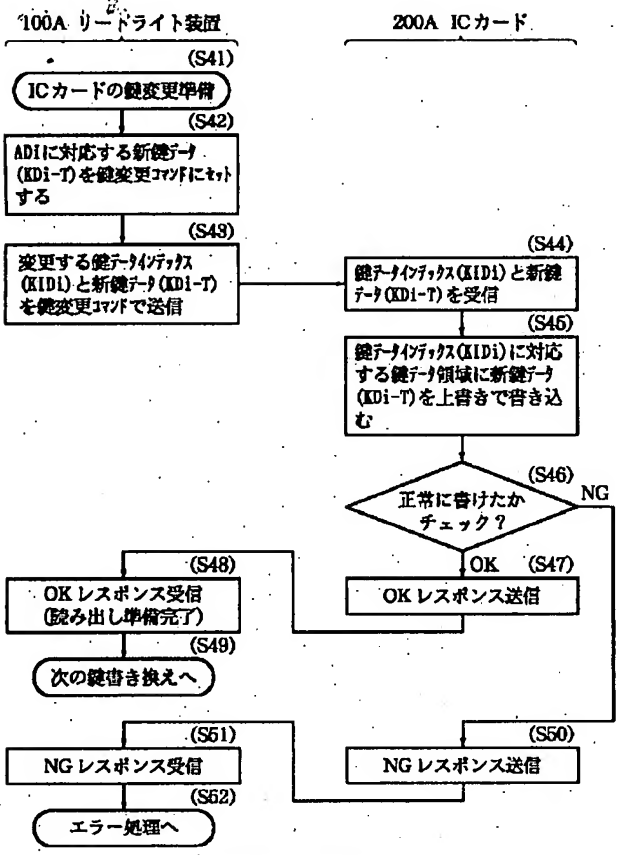
[Drawing 5]



[Drawing 6]



[Drawing 7]



上記手順を変更する鍵の個数くりかえす

[Translation done.]